AUTHENTICATING WITHOUT OPENING ELECTRONIC MAIL

FIELD OF THE INVENTION

The present invention relates to the field of electronic mail, and more particularly to a method for authenticating electronic mail that does not require opening the electronic mail, so that mail which carries a computer virus may be identified and rejected prior to opening.

BACKGROUND

Computer viruses initiated by electronic vandals are now responsible for the loss of untold hours of labor. In many cases, these viruses are spread as attachments to electronic mail (e-mail). When a recipient opens e-mail initiated by a vandal, and then opens the attachment, the virus is unleashed to do its damage. For this reason, experienced computer users are sometimes reluctant to open e-mail attachments.

Consequently, electronic vandals often go to great lengths to give their e-mail a veneer of legitimacy, often by fraudulently stating the identity of its originator. For example, a virus may gain access to the address book of a first computer user, and propagate itself, under the assumed identity of the first computer user, to a number of recipients who have come to trust the integrity of e-mail received from the first computer user. Still, when the virus is carried by an attachment to e-mail, the recipient may open the e-mail and inspect the attachment outwardly without taking

undue risk. Upon inspection, the odd nature of malevolent attachments, for example their use of odd file types, may alert the recipient to the true purpose of the e-mail, and the recipient may discard the e-mail without opening the attachment and therefore without sustaining any damage.

Unfortunately, vandals have now developed viruses that may be carried directly by e-mail, and do not require transport in an attachment. When a victim receives such an e-mail that fraudulently purports to originate from a trusted source, the victimized recipient may instinctively open the e-mail and thereby contract the virus. Thus, there is a need for a method of authenticating e-mail – verifying that the e-mail indeed originates from the source whose identity it bears, and may therefore be presumed virus-free – which does not require that the recipient open the e-mail.

SUMMARY

The present invention provides a way of authenticating electronic mail (e-mail) that does not require the recipient to open the e-mail, so that the recipient may guard against computer viruses that become active when electronic mail is opened.

An originator and a recipient agree beforehand on a privately held authentication key, such as a simple natural-language phrase, which identifies the originator to the recipient. The originator prepares e-mail addressed to the recipient. The originator reads the authentication key from a memory, for example a database. The authentication key is included in a field of the e-mail that

can be examined by the recipient without opening the e-mail, which is called here an open field, and which may be, for example, the subject line of the e-mail. The e-mail is then sent from the originator to the recipient.

When the recipient receives the e-mail, the recipient identifies the originator by examining a source identifier of the e-mail, for example its from address. The recipient determines whether an authentication key is expected to be present in e-mail that bears the particular source identifier. If an authentication key is expected to be present but is in fact not present, the recipient may reject the e-mail. If an authentication key is present, the recipient determines whether the authentication key that is present is the earlier-agreed authentication key associated with the originator. If the authentication key present is the earlier-agreed authentication key, the recipient may open the e-mail. If the authentication key present is not the earlier-agreed authentication key, the recipient may reject the e-mail.

Thus, the present invention enables the recipient of e-mail to authenticate the purported originator of the e-mail without opening the e-mail, and consequently enables the recipient to reject e-mail that fraudulently bears the identifier of a trusted originator and yet carries a computer virus that would otherwise activate were the recipient to open the e-mail. These and other aspects of the invention will be more fully appreciated when considered in light of the following detailed description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram that shows structural aspects of an exemplary embodiment of the invention.

FIG. 2 is a flowchart that shows aspects of the operation of an exemplary embodiment of the invention.

DETAILED DESCRIPTION

The present invention enables a recipient of electronic mail (e-mail) to authenticate the purported originator of the e-mail without opening the e-mail, and consequently enables the recipient to reject e-mail that fraudulently bears the identifier of a trusted originator and yet carries a computer virus that would otherwise activate were the recipient to open the e-mail.

FIG. 1 is a block diagram that shows structural aspects of an exemplary embodiment of the invention. In the exemplary embodiment of FIG. 1, an originator 100 prepares e-mail for sending to a recipient 150. The originator 100 may include an e-mail terminal 110 suitable for use by a human, such as a personal computer, a personal digital assistant, limited-function apparatus for supporting e-mail, an e-mail-enabled cellular telephone, and the like. The originator 100 may include a post-processor 120 for executing certain aspects of the present invention as will be described. Although the post-processor 120 is shown in FIG. 1 for descriptive convenience as

being separate from the e-mail terminal 110, the post-processor 120 may be integrated with the e-mail terminal 110. For example, the post-processor 120 may be software that is executed by the e-mail terminal 110. Also shown in FIG. 1 is an originator's memory 130, which may be a single register, a multi-register structure, a database, and so forth. Although the originator's memory 130 is shown in FIG. 1 for descriptive convenience as being separate from the e-mail terminal 110 and the post-processor 120, the originator's memory 130 may be internal to the e-mail terminal 110 or the post-processor 120.

The originator 110 is connected to the recipient 150 by the Internet 190 or other communication network, which other communication network may be local-area or wide-area in its coverage.

The recipient 150 may include an e-mail terminal 170 suitable for use by a human, such as a personal computer, a personal digital assistant, limited-function apparatus for supporting e-mail, an e-mail enabled cellular telephone, and the like. The recipient 150 may include a pre-processor 160 for executing certain aspects of the present invention as will be described. Although the pre-processor 160 is shown in FIG. 1 for descriptive convenience as being separate from the e-mail terminal 170, the pre-processor 160 may be integrated with the e-mail terminal 170. For example, the pre-processor 160 may be software that is executed by the e-mail terminal 170. Also shown in FIG. 1 is a recipient's memory 180, which may be a single register, a multi-register structure, a database, and so forth. Although the recipient's memory 180 is shown in FIG. 1 for descriptive convenience as being separate from the e-mail terminal 170 and the pre-processor 160, the recipient's memory 180 may be internal to the e-mail terminal 170 or the pre-

processor 160.

FIG. 2 is a flowchart that shows aspects of the operation of an exemplary embodiment of the invention. Before the originator 100 prepares the e-mail, the originator 100 and the recipient 150 agree on an authentication key that identifies the originator 100 to the recipient 150 (step 200). The authentication key may be a natural-language word or a natural-language phrase, although this is not a limitation of the invention, as the authentication key may be any set of alphanumeric or other characters. For example, an authentication key might be the word "asparagus," or the phrase "the truth shall make you free," or the character string "xx6$jdf," and so forth. The authentication key may be dependent upon only the identity of the originator 100, or may depend on the identity of both the originator 100 and the recipient 150. In an example of the former kind of dependence, an originator might use the authentication key "ABC" when preparing e-mail for any recipient, whereas, in an example of the latter kind of dependence, another originator might use the authentication key "DEF" when preparing e-mail for a first recipient, and use the authentication key "GHI" when preparing e-mail for a second recipient. In the former case, the authentication key is associated with only the originator 100; in the latter case, the authentication key associated with the originator 100 is further associated with the recipient 150.

The authentication key may be provided *a priori* to the originator 100 and the recipient 150. The originator 100 may store the authentication key in the originator's memory 130, and the recipient may store, in the recipient's memory 180, the authentication key along with an indicator, such as

a flag, which indicates whether e-mail from the originator 100 is expected to include an authentication key. Optionally, the authentication key may be stored encrypted in either memory or in both.

The e-mail terminal 110 of the originator 100 prepares e-mail for sending from the originator 100 to the recipient 150 (step 205). The post-processor 120 accepts the e-mail from the e-mail terminal 110, reads the authentication key from the originator's memory 130, and includes the authentication key in an open field of the e-mail (step 210). Optionally, inclusion of the authentication key may be responsive to an automatic prompt by the post-processor 120 through the e-mail terminal 110, followed by manual authorization by a human using the e-mail terminal 110. The address of the location from which the authentication key is read in the originator's memory 130 may be dependent upon an identifier of the recipient 150, for example arithmetically dependent upon the to-address of the e-mail. The open field of the e-mail may be any field that the recipient 150 can access without opening the e-mail, for example the subject line of the e-mail, and may be visible to a human viewing the recipient's e-mail terminal 170 or may be hidden from view.

The e-mail with authentication key is sent from the originator 100 to the recipient 150 (step 215), and the recipient 150 receives the e-mail (step 220).

Upon receipt of the e-mail by the recipient 150, the pre-processor 160 determines whether an authentication key should be expected to be present in the open field of the incoming e-mail (step

225). To make this determination, the pre-processor 160 may access the recipient's memory 180, looking for the indicator which indicates whether e-mail from the originator 100 is expected to include an authentication key. If an authentication key is not expected to be present in the open field, the pre-processor 160 may accept the e-mail (step 230). To accept the e-mail and to reject the e-mail are complements here – e-mail that is accepted by the pre-processor 160 is simply e-mail that is not rejected by the pre-processor 160, and acceptance by the pre-processor 160 carries no implication that the e-mail will necessarily be opened.

Otherwise (i.e., an authentication key is expected to be present in the open field), the pre-processor 160 examines the open field and determines whether an authentication key is present (step 235). If an authentication key is not present in the open field, the pre-processor may reject the e-mail (step 240). E-mail that is rejected may be discarded automatically, or may be retained but marked as suspicious so that a human may decide whether to open or to discard the e-mail.

Otherwise (i.e., an authentication key is present in the open field), the pre-processor 160 determines whether the authentication key present in the open field is associated with the originator 100 (step 245), i.e., the authentication key present is the same as the agreed authentication key which was earlier stored in the originator's memory 130 and the recipient's memory 180. To make this determination, the pre-processor 160 may access the recipient's memory 180 at a location dependent upon an indicator that identifies the originator 150, such as the e-mail's from-address, read the authentication key stored earlier, and compare the authentication key present with the authentication key stored earlier.

If the authentication key present in the open field is associated with the originator, i.e., the authentication key present is the same as the authentication key stored earlier, the pre-processor 160 accepts the e-mail (step 230). Otherwise (i.e., the authentication key present in the open field is not associated with the originator), the pre-processor 160 rejects the e-mail.

In another embodiment of the invention, which may not require the use of the post-processor 120 or the pre-processor 160, the authentication key may be recalled by a first human who uses the e-mail terminal 110 to manually enter the authentication key in an open field of the e-mail, for example on the subject line of the e-mail. Upon receipt of the e-mail by a second human, the second human may determine whether the authentication key associated with the originator appears in the open field, and decide accordingly whether to open the e-mail or not.

From the foregoing description, those skilled in the art will appreciate that the present invention provides an authentication method that enables a computer user to guard against a computer virus that is carried in e-mail with a fraudulent identifier such as a fraudulent from-address and which becomes active upon opening the e-mail. The foregoing description is illustrative rather than limiting, however, and the scope of the present invention is limited only by the following claims.